Access Control System

with

Hand Geometry Verification

and

Smart Cards

Rand Sanchez-Reillo and Ana Gonzalez-Marcos
E.T.S.I. Telecommunicacion

ABSTRACT

An access control system that joins the uniqueness of biometric verification, as well as the storage security and processing capabilities of smart cards, is defined here. The biometric technique chosen has been hand geometry, which is considered to provide low/medium security (there are other much more secure, as fingerprint, iris or retina), to be easy to use, to achieve high acceptance by users, and which performance is given throughout fast processing and medium cost. Also, the small template size needed for each user is positive for storage and processing capabilities required in the system. But the innovation in the system proposed is that the smart card not only stores the user's template, but also performs the verification process with the features set by the terminal to the card. With this improvement, the security of the system has risen because the template is never extracted from the card, avoiding duplication of such sensible data. The specifications for the enrollment process will be presented as well as the applications where this new system is recommended.

Authors' Current Address:
R. Sanchez-Reillo and A. Gonzalez-Marcos, E.T.S.I. Telecommunicacion, Dept. Tecnologia Fotonica, Ciudad Universitaria, s/n; E-28040, Madrid, Spain.

Based on a presentation at Carnahan '99.

INTRODUCTION

Most of the access control systems implanted nowadays are based in PIN (Personal Identification Number) presentation and/or Magnetic Stripe Cards. These solutions, although secure enough for most applications, could not be valid for some high security environments. This lack of security is led by the possibility of forgetting the PIN and/or losing or duplicating the card. Industry is solving this problem by applying new technologies like smart cards and biometric recognition. Smart cards [13] solve the duplication problem and ease management of lost cards, but the user must remember a PIN in order to be verified by the system. This means that if a user has more than one card, he must remember as many different PINs as cards owned, which leads to the common practice of applying the same PIN to all cards, with the loss of security that this practice achieves. Biometric identification solves the problem of remembering several PINs, as this number is transformed into biological features of the user [4].

But before designing or selecting a biometric access control system, two aspects must be defined: the biometric technique used; and the configuration of the system. The selection of the biometric technique is not trivial. There

are several techniques (fingerprint, voice, f[illegible] iris, retina, hand, signature, etc. [4, 5]), and its selectio[illegible]ould be made by means of security level, cost, environment, user interaction, user acceptance and verification time. The configuration of the system can be as a recognition system (comparing the features extracted with the templates of all users stored in a database), or as a verification system (comparing the features extracted to the template of the user who claims his identity). A recognition system requires a central database and communication of all POAs (Points of Access) with that database. A verification system can avoid the need of such a database and connections, by using a portable storage media, where the user's template is recorded.

FEATURES EXTRACTION

From the biometric techniques existing today, hand geometry has been selected [9]. Hand geometry is considered a low/medium security technique, what can lead to take it out of consideration, compared to much more secure techniques such as fingerprint, iris or retina. But hand geometry has several advantages that are interesting for developing an access control system. These advantages are:

- Medium cost (only a low/medium resolution CCD camera is needed).
- Fast computation (low computational cost and immediate result obtained).
- Low template size (the lowest of all techniques known today).
- Very easy to use and attractive to users.
- Easy to clean and maintain.
- Lack of relation to police, justice and criminal records.

All these characteristics makes this technique attractive for systems integrators, due to its low overall cost, and as well very quickly accepted by users who do not see any inconvenience in the system.

The user's features extraction is based on a photograph of the top and side of the user's hand taken by a CCD medium resolution camera. To obtain the photograph, the user must place his hand in a platform with 6 tops (Figure 1), which guide the position of the palm. When the pressure sensors located in each of the tops are activated, the photograph is taken (Figure 2).

After that, a simplified morphological and volumetric image processing is performed with the photograph, based on simple algorithms [3, 6, 10, 11]. Several measurements are taken, including finger widths at several points, palm width, deviation of the fingers from the straight line, location of the interfinger points, angles between them, palm height, etc. From all those features extracted, a set is selected for verification purposes. This

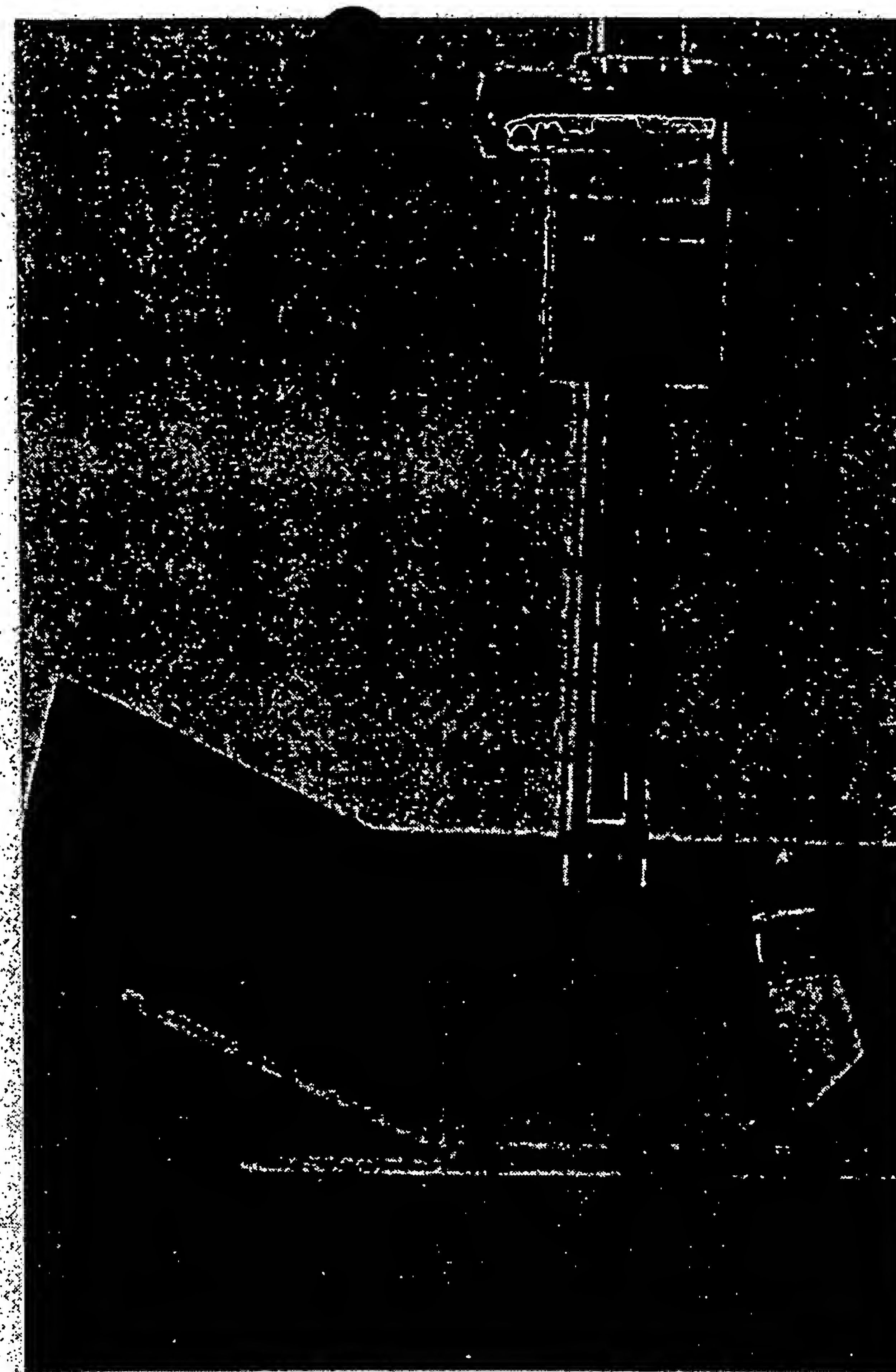

Fig. 1. Platform Prototype

Fig. 2. Sample Photograph

selection has been performed through inter-class/intra-class deviation ratio. Once the features with the highest ratio are detected, a principal component analysis has been performed to reduce the dimension of

the feature vector [1-12]. The structure of the feature vector obtained through this analysis, is applied to all the users and, therefore, the feature vector for each user sample is represented by 13 bytes.

VERIFICATION

Several methods for the verification process have been studied [10]. From those methods, three are presented as the most representative:

- *Euclidean Distance:* Verification is performed calculating the Euclidean distance between the template of the user and the sample taken, and comparing it with a threshold value. The template is obtained as the mean value of the first five photographs taken from that user in the enrollment process.
- *Hamming Distance:* The number of features out of the mean, plus/minus a factor of the standard deviation, is counted and compared to a threshold. The template is obtained as the mean and standard deviation of the five first photographs taken from the user in the enrollment process.
- *Gaussian Mixture Modelling (GMM):* The user's sample is entered in the GMM and the likelihood probability is obtained. The GMM of each user is composed of a set of means, variances and weights, tuned with the enrollment samples (five). This technique has been widely used in Speaker Recognition, as it can be seen in [2, 7, 8].

Among the other methods studied, a neural network approach through Radial Basis Functions [12] was tried. It showed very good results in classification, i.e., having a central database with all users enrolled in the system. But in order to use this approach in verification, a set of other users should be used in the enrollment process. This fact goes against the philosophy of the biometric system explained here, as the existence of a central database is to be avoided.

The success of the verification scheme is obtained by two ratios: False Acceptance Ratio (FAR) and False Rejection Ratio (FRR). These two ratios are complementary, in the sense that if a reduction in FAR is needed, then an increase in FRR is obtained. Results obtained are presented in the following table targeting a

	FAR	FRR	Template size
Euclidean	23%	19%	13 bytes
Hamming	16%	9%	26 bytes
GMM	6,6%	9%	153 bytes

FRR near 10%. Twe[illegible]sers and at least ten samples of each user participated in the calculation of ratios.

From the figures obtained, several conclusions can be drawn. While the Euclidean Distance gives the lowest template size, its performance is quite poor, not being able to obtain low error rates easily. On the other hand, GMM shows really good results, comparable to the ones obtained for other, so claimed, high security biometric techniques; but the template size is significantly increased. Half the way, the Hamming Distance provides nice error rates, maintaining a very low template size.

SMART CARDS

Biometric Authentication Systems based in hand geometry or other techniques are available, even commercially, and with great success. But these kinds of systems present a lack of security due to the way of storing the template and verifying the user's sample. Not considering the systems based in a central database where the users' templates are stored, other systems use a portable storage media to keep and transmit the template. Examples of this media could be any memory based scheme, such as magnetic stripe cards, laser cards or integrated circuit cards. With this system configuration the verification is performed in the terminal, therefore, needing the terminal to extract the user's template from the card.

The solution presented is analog to the advance that smart cards meant about PIN verification, compared to magnetic stripe cards. In smart cards, the PIN is verified inside the card, not being able to read the PIN from the card, avoiding duplication of the user's card. The system proposed compares inside the card, the user's sample with the template stored.

To achieve this goal, a new data structure must be present in the card, as well as new commands for writing, updating, and verifying the template. JavaCards have been used to develop the prototype in order to test the technology and, after a successful pilot project, to manufacture in hard masking.

The three verification methods selected have been tested, obtaining the following figures:

	Verification Time	Code Size
Euclidean	0.3 seconds	372 bytes
Hamming	0.2 seconds	428 bytes
GMM	2.1 seconds	3873 bytes

With these results and those shown in the verification analysis, it seems that the Hamming Distance

gives the best performance ratio between Failures (FAR and FRR), code size and verification time. But if high security is necessary, GMM is recommended, although deep work should be done to decrease the verification time obtained nowadays.

ACKNOWLEDGEMENTS

The authors thank Professor Jose A. Martin-Pereda and Assistant Professor Carmen Sanchez-Avila for their support and corrections of the work done. It is necessary to thank all the users who took part in the experiments.

In memory of Assistant Professor Jose L. Zoreda-Bartolome, teacher, innovator, researcher and friend.

REFERENCES

[1] Duda, R.O. and Hart, P.E., 1973, Pattern Classification and Scene Analysis, John Wiley & Sons, Inc.

[2] Gonzalez-Rodriguez, J., Cruz-Llanas, S. and Ortega-Garcia, J., October 1999, Biometric Identification through Speaker Verification over Telephone Lines, Proceedings of the 33rd Annual International Carnahan Conference on Security Technology. Madrid, Spain, pp. 238-242.

[3] Jain, A.K., 1988, Fundamentals of Digital Image Processing, Prentice Hall.

[4] Jain A.K., Bolle R. and Pankanti, S., et al., 1999, Biometrics: Personal Identificacion in Networked Society, Kluwer Academic Publishers.

[5] Jain, L.C., Halici, U., Hayashi, I., Lee S. B. and Tsutsui S., 1999, Intelligent Biometric Techniques in Fingerprint and Face Recognition, CRC Press LLC.

[6] Jähne, B., 1997, Practical Handbook on Image Processing for Scientific Applications, CRC Press LLC.

[7] Reynolds, D.A. and Rose, R.C., 1995, Robust Text Independent Speaker Identification Using Gaussian Mixture Speaker Models, IEEE Trans. on Speech and Audio Processing, Vol. 3, Int'l, pp. 72-83.

[8] Ruiz, B., Domingo, P. and Hernandez, L., October 1999, A Dual Speech/Speaker Recognition using GMM in Speaker Identification and a HMM in Keyword Speech Recognition, Proceedings of the 33rd Annual International Carnahan Conference on Security Technology. Madrid, Spain, pp. 251-254.

[9] Sanchez-Reillo, R. and Gonzalez-Marcos A., October 1999, Access Control System with Hand Geometry Verification and Smart Cards, Proceedings of the 33rd Annual International Carnahan Conference on Security Technology. Madrid, Spain, pp. 485-487.

[10] Sanchez-Reillo, R., Sanchez-Avila, C. and Gonzalez-Marcos A., 1999, Multiresolution Analysis and Geometric Measure for Biometric Identification, CORE Secure Networking. Dusseldorf, Germany.

[11] Schalkoff, R.J., 1989, Digital Image Processing and Computer Vision, John Wiley & Sons, Inc.

[12] Schürmann, J., 1996, Pattern Classification. A unified view of statistical and neural approaches, John Wiley & Sons, Inc.

[13] Zoreda, J.L. and Oton, J.M., 1994, Smart Cards, Artech House, Inc.

Electronic Parts & Packaging for Space and Aeronautic Applications

IMAPS will join forces with the NASA Electronic Parts & Packaging (NEPP) Program to cosponsor this advanced technology workshop on April 3-5, 2000, in Washington, DC.

The proposed workshop on Electronic Parts and Packaging for Space and Aeronautic should be an ideal opportunity for those in the aerospace industry and academia to participate in review and discussion of the latest advances in this fascinating and demanding area of micro-electronics and packaging. This event provides technical interaction and education in the micro-electronics and packaging industries. The three-day, five-session workshop will represent a condensed assessment of novel, state-of-the-art electronic parts and packaging technologies for space and aeronautic applications.

The NEPP Program is funded by NASA Headquarters with the charter to assess new and advanced electronic parts and packaging technologies for space and aeronautic applications. The Lead Center for this activity is JPL. There are three technical projects within NEPP: Electronic Parts; Electronic Packaging; and Electronic Radiation Characterization. For details, contact: Ann Bell at (703) 758-5166; E-mail: (abell@imaps.org).